Amendment to Claims

Please amend claims 1, 7 and 13.

1. (Currently Amended) A system for a physical entity for authenticating that a user access request to the system is generated from a client system close to the physical entity, comprising

a web server for providing web content designed for an access request from the client system close to the physical entity;

a location beacon adjacent to the physical entity to transmit within a predetermined transmission range a first beacon signal containing a web address of the web server and a location token for indicating physical presence of the client system close to the physical entity and which ~~that~~ expires within a predetermined time period;

a location authentication module for authenticating that the client system having received the first beacon signal is still close to the physical entity wherein the location authentication module receives a first request including the web address, the location token, and ~~the key~~ a key from the client system;

a location authentication beacon adjacent to the physical entity and communicatively coupled to the location authentication module for receiving the key and the location token and for encrypting a customized location token that expires in a predetermined time period using the key and for transmitting a second beacon signal within the predetermined transmission range containing the web address and the customized token; and

responsive to receiving a second request from the client system including the customized token and the web address, the location authentication module causes the web server to provide content designed for an access request from the client system close to the physical entity if the customized location token has not expired.

2. (Previously Presented) The system of claim 1, wherein responsive to the location token in the first request being expired, the location authentication module causes the web server to provide web content designed for an access request from a client system not close to the physical entity.

3. (Previously Presented) The system of claim 1, wherein the customized token also expires within a predetermined time period, wherein if the location authentication module determines that the customized token has expired, then the location authentication module does not cause the web server to service the second request.

4. (Previously Cancelled.)

5. (Previously Presented) The system of claim 1, wherein the key is a random number generated by the client system.

6. (Previously Presented) The system of claim 1, wherein the location authentication beacon further comprises

a first token generator that generates the un-encrypted customized token using a stored secret key;

a second token generator that encrypts the customized token using a random number key;

a store that stores the customized token and the web address;

a communication interface that receives the web address and the customized token from the store and transmits the second beacon signal.

7. (Currently Amended) A system for authenticating the location of a client system accessing a web server system for a physical entity, comprising

in the web server system,

a location beacon adjacent to the physical entity to transmit within a predetermined transmission range a first beacon signal containing a web address of the web server system and a location token for indicating physical presence of the client system close to the physical entity and which ~~that~~ expires within a predetermined time period;

a location authentication module for authenticating that the client system having received the first beacon signal is still close to the physical entity wherein the location authentication module receives a first request including the web address, the location token, and ~~the key~~ a key from the client system;

a location authentication beacon adjacent to the physical entity and communicatively coupled to the location authentication module for receiving the key and the location token and for encrypting a customized location token that expires in a

predetermined time period using the key and for transmitting a second beacon signal within the predetermined transmission range containing the web address and the customized token;

responsive to receiving a second request from the client system including the customized token and the web address, the location authentication module causes the web server to provide content designed for an access request from the client system close to the physical entity;

in the client system,

a random number generator that generates the key; and

a beacon receiver that receives the first and second beacon signals,

wherein the beacon receiver generates the first request that includes the key and sends the customized token to a web browser of the client system such that authenticity and location of the client system is verified.

8. (Previously Presented) The system of claim 7, wherein responsive to the location token in the first request being expired, the location authentication module causes the web server to provide web content designed for an access request from a client system not close to the physical entity.
9. (Original) The system of claim7, wherein the customized token also expires within a predetermined time period, wherein if location authentication module determines that the customized token has expired, then the location authentication module does not cause the web server to service the second request.
10. (Previously Cancelled.)
11. (Original) The system of claim 7, wherein the beacon receiver further comprises

a receiver circuit that receives the beacon signals and parse the tokens from the beacon signals;

a processor coupled to the receiver circuit to control the receiver circuit to either receive the first beacon signal or the second beacon signal;

a request generation module that generates the first request that contains the key.

12. (Original.)The system of claim 7, wherein the location authentication beacon further comprises

a first token generator that generates a token using a stored secret key;

a second token generator that encrypts the token using the random number key such that the encrypted token becomes the customized token;

a store that stores the customized token and the web address;

a communication interface that receives the web address and the customized token from the store and transmits the second beacon signal.

13. (Currently Amended) A method of authenticating the location of a client system accessing a web server system associated with a physical entity, comprising

transmitting within a predetermined transmission range a first beacon signal containing a web address of the web server system and a location token for indicating physical presence of the client system close to the physical entity and which ~~that~~ expires within a predetermined time period from a location beacon adjacent to the physical entity;

generating a random number key in the client system close to the physical entity and sending a first request from the client system to the web server system responsive to the client system receiving the first beacon signal, wherein the first request contains the web address, the location token and the key;

retrieving the key from the first request in the web server system if the location token has not expired and encrypting a customized token that expires in a predetermined time period using the key;

transmitting a second beacon signal within the predetermined transmission range containing the web address and the customized token from a location authentication beacon adjacent to the physical entity; and

decrypting the customized token in the client system using the key to determine if the second beacon signal is intended for the client system.

14. (Previously Presented) The method of claim 13, further comprising

sending a second request to access the web server system if the customized token can be decrypted in the client system using the key, wherein the second request contains the web address of the web server system and the customized token;

causing the web server system to provide content designed for an access request from a client system close to the physical entity responsive to the

second request if the customized token in the second request has not expired; and

causing the web server system not to service the second request if the customized token in the second request has expired.

15. (Previously Cancelled.)